UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/653,966	09/01/2000	Daniel R. Salmonsen	003551.P015	5668

7590 07/28/2005

Blakely Sokoloff Taylor & Zafman LLP
12400 Wilshire Boulevard
Seventh Floor
Los Angeles, CA 90025-1026

EXAMINER	
SIMITOSKI, MICHAEL J	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 07/28/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/653,966	SALMONSEN ET AL.	
	Examiner	Art Unit	
	Michael J. Simitoski	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 April 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-26* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-26* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. The response of 4/27/2005 was received and considered.

2. Claims 1-18 & 20-26 are pending.

Response to Arguments

3. The Abstract submitted 10/27/2004 is accepted.

4. On p. 9, ¶3 of Applicant's response (unless otherwise specified, filed 10/27/2004), Applicant states that the Office Action indicated that 8, 15, 16, 19 & 22 were objected to as being allowable if rewritten. However, claims 15 & 16 were not indicated as such.

5. In light of Applicant's response (p. 9, ¶4-5), the objection to claims 1-25 due to reference characters is withdrawn and the rejection of claim 1 under 35 U.S.C. §112 ¶1 is withdrawn.

6. Regarding Applicant's response (p. 10, ¶6 – p. 11, ¶1), it is noted that Applicant has overcome the rejection of claim 1 under 35 U.S.C. §112 ¶2, but not the rejections of claims 2, 7 & 17-24. Those rejections are reiterated below.

7. The indicated allowability of claims 8 & 19 is withdrawn in view of the newly discovered reference(s) to Menezes. Rejections based on the newly cited reference(s) follow. Further, in light of a newly discovered indefiniteness issue, the allowability of claim 22 is withdrawn. Accordingly this Office Action is made non-final.

8. Applicant's arguments with respect to claims 1-18 & 22-25 (p. 10, ¶2 – p. 11, ¶2) have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 112

9. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

10. Claims 2, 7-9 & 17-24 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

a. Regarding claim 2, it is unclear how claim 2 relates to claim 1, as there is nothing to tie claim 2 to claim 1. Claim 3 is rejected based upon its dependence on claim 3.

b. Regarding claim 3, the claim recites the limitation "the application" in line 2 of the claim. There is insufficient antecedent basis for this limitation in the claim.

c. Regarding claim 3, it is unclear whether "the content" is referring to "the content" recited in claim 1 or the encrypted content recited in claims 2-3.

d. Regarding claim 7, it is unclear whether "the content" is referring to "the content" recited in claim 1 or the encrypted content recited in claims 2-3.

e. Regarding claim 7, the claim recites the limitation "the application" in line 2 of the claim. There is insufficient antecedent basis for this limitation in the claim.

f. Regarding claim 8, it is unclear whether the "session key" in claim 8 refers is the same session key as in claim 1 or an additional session key.

g. Regarding claim 8, it is unclear whether "the ... session key" refers to the one-time session key of claim 8 or the session key of claim 1.

h. Regarding claim 10, the phrase "or another type" renders the claim(s) indefinite because the claim(s) include(s) elements not actually disclosed (those encompassed by

"or another type"), thereby rendering the scope of the claim(s) unascertainable. See MPEP § 2173.05(d).

i. Regarding claim 17, it is unclear whether more than one "read ... content" is occurring because the step of reading appears to happen twice (line 3 and line 7). Claims 18-24 are rejected based upon their dependency upon claim 17.

j. Regarding claim 20, it is unclear whether "the key" (last line) is referring to the decryption key or the session key, as both are used to decrypt the data, according to the specification.

k. Regarding claim 20, the claim recites the limitation "the data" in line 4 of the claim. There is insufficient antecedent basis for this limitation in the claim.

l. Regarding claim 21, the claim recites "wherein the decryption key is a session key and a content decryption key" rendering the claim indefinite because the claim 17 recites a session key; therefore it is unclear whether "a session key" in claim 21 refers to the session key in claim 17 or an additional session key.

m. Regarding claim 22, it is unclear whether "a session key" (line 3) is the same session key as previously mentioned in claim 17, or an additional one.

n. Regarding claim 22, "an encryption logic to return the session key" implies returning the key to the sender, however, the specification describes the session key being returned to the host/client system; therefore the claim language is unclear.

o. Regarding claim 22, "the session key" (line 7) could refer to "a session key" recited in claims 22 or 17.

p. Regarding claim 25, the claim recites the limitation "the server" in lines 5-19 of the claim. There is insufficient antecedent basis for this limitation in the claim.

q. Regarding claim 25, the claim recites the limitation "the disk ID" in lines 13-19 of the claim. There is insufficient antecedent basis for this limitation in the claim.

r. Regarding claim 25, it is unclear whether "an application" (line 8) and "an application" (line 9) refer to the same application.

s. Regarding claim 25, the claim recites the limitation "the data" in line 11 of the claim. There is insufficient antecedent basis for this limitation in the claim.

t. Regarding claim 25, it is unclear to which "user", recitations of the limitation "the user" (lines 16-19) are referring.

u. Regarding claim 25, the claim recites the limitation "the user authentication data" in lines 15-19 of the claim. There is insufficient antecedent basis for this limitation in the claim.

v. Regarding claim 25, it is unclear to which "data" the recitations of "the data" (lines 22-24) are referring.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-6 & 10-16 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent 6,499,106 to Yaegashi et al. (**Yaegashi**) in view of Handbook of Applied Cryptography by Menezes et al. (**Menezes**).

Regarding claim 1, Yaegashi discloses determining a secure medium identification (disk ID) from a secure medium (col. 10 lines 47-65) including content/sensitive information (col. 8 lines 61-67), sending the ID to a server/central access control system (col. 9 lines 20-28), requesting user authentication (col. 10 lines 47-65), and if the user is successfully authenticated, receiving a session key/decryption key from the server to enable reading of the content on the secure medium (col. 11 lines 1-22). Yaegashi lacks the session key being encrypted and receiving a decrypted copy. However, Menezes teaches that a key translation center is a server to establish trusted communications where A sends a message to the server, encrypted with the servers key, where it is decrypted with the server's key, re-encrypted with the recipients key and delivered to the recipient (pp. 553-554). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Yaegashi to encrypt the session key and send it to the server, where it would be decrypted and the decrypted copy re-encrypted and sent to the user if the user is authenticated. One of ordinary skill in the art would have been motivated to perform such a modification to communicate between two entities without sharing an initial key between the two, as taught by Menezes (pp. 553-554).

Regarding claims 2 & 3, Yaegashi discloses streaming/sending the content to an application/information access system that uses the session key/decryption key to decrypt and display the content (col. 11 lines 12-22).

Regarding claim 4, Yaegashi discloses the content stored as encrypted content on the secure medium (col. 11 lines 1-22).

Regarding claims 5 & 6, Yaegashi discloses receiving a content decryption key from the server, in response to the disk ID/disc identification information and the user authentication (col. 10 lines 47-65) wherein the content decryption key is determined based on the disk ID/disc identification information (col. 12 lines 29-50).

Regarding claim 10, Yaegashi discloses a CD (col. 11 lines 1-22).

Regarding claim 11, Yaegashi discloses digitally encoded music (col. 1 lines 44-59 & col. 4 lines 17-41).

Regarding claim 12, Yaegashi discloses the use of a credit card for unlocking of copy-protected software, but lacks specific disclosure of using a credit card for authentication. However, official notice is hereby taken that it was well-known in the art to authenticate online purchases based on a credit card to allow royalties to be collected. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to authenticate via credit card. One of ordinary skill in the art would have been motivated to perform such a modification to allow royalties to be collected as was well-known in the art.

Regarding claim 13, Yaegashi discloses a password used for authentication (col. 10 lines 47-65).

Regarding claim 14, Yaegashi discloses determining if the disk ID is already associated with a user (col. 12 lines 4-17) and if the disk ID/disc identification information is not yet associated with the user, associating the user authentication data/login identity with the disk ID/disc identification information (col. 12 lines 4-17 & lines 56-61).

Regarding claim 15, Yaegashi discloses determining that the current user authentication matches the user (validation/authentication by determining if the user matches a key for the current disk) (col. 10 lines 47-65 & col. 12 lines 4-8) in addition to determining if a user is associated with the disk ID/disc identification information (col. 12 lines 4-17).

Regarding claim 16, Yaegashi discloses that if validation is unsuccessful, the session key/content key is not returned (col. 11 lines 5-10).

4. Claims 17 & 18, as best understood, are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent 6,636,966 to Lee et al. (**Lee**) in view of U.S. Patent 6,236,727 to Ciacelli et al. (**Ciacelli**) in further view of Applied Cryptography, Second Edition by **Schneier**.

Regarding claim 17, Lee discloses a reader/data storage engine (Fig. 1 #14) to read an identification (ID)/identification of content to enable (Fig. 3A #31) and content/data stored on a storage medium (col. 2 lines 49-67), encryption logic (Fig. 2C'1) to send the identification to a server/content key server (col. 9 lines 17-26) in encrypted form (col. 9 lines 39-46), an authentication logic to receive authentication from the server/content key server indicating approval to read the content of the secure medium/storage medium (col. 9 line 63 – col. 10 line 3) and sending the content to an application/host (Fig. 2C'1 & Fig. 2B #254). Lee lacks the encryption logic encrypting the content prior to sending the content to an application/host. However, Ciacelli teaches the well-known concept that encrypting a data stream, one ensures that the information in the stream (such as copyrighted material) is not exposed during the data transfer (col. 3 lines 25-64). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to encrypt the content prior to sending the content to

an application. One of ordinary skill in the art would have been motivated to perform such a modification to ensure that the content is not exposed during data transfer, as taught by Ciacelli (col. 3 lines 25-64). As modified, Lee lacks session key generation logic to generate a one-time session key and sending the session key encrypted to a server. However, Schneier teaches that session keys are used to secure a single conversation (p. 180) and are usually first exchanged and then used (p. 33) because symmetric encryption is faster (p. 33). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to generate a one-time session key and send it encrypted to the server. One of ordinary skill in the art would have been motivated to perform such a modification to secure the conversation, including the received authentication, with high-speed cryptography, as taught by Schneier (pp. 33 & 180).

Regarding claim 18, Lee discloses using a symmetric key to encrypt the ID/packet (col. 11 lines 38-53).

5. Claims 20 & 21, as best understood, are rejected under 35 U.S.C. 103(a) as being unpatentable over **Lee**, **Ciacelli** & **Schneier**, as applied to claim 17 above, in further view of **Yaegashi**.

Regarding claim 20, Lee discloses receiving a decrypting key from the server and discloses the possibility of requesting a payment with a credit card/authentication (col. 5 lines 54-67), but lacks explicitly authenticating a user and streaming decryption logic to receive data from the server and play the data. However, Yaegashi teaches a similar system for the distribution of information on a media where a user must log in to the information access system/system that reads the recording medium (col. 10 lines 46-65). While Yaegashi does not

explicitly teach motivation for doing so, it is well-known in the art to use a user identification and password to identify/verify/authenticate a user to another entity, as taught by Schneier (page 52). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to provide a user authentication interface to request a user authentication password in response to a server request, and to send the data received from a user to the server, receiving a decryption key from the server if the user is authenticated, as suggested by Lee (col. 5 lines 54-67) and Yaegashi (col. 10 lines 46-65). One of ordinary skill in the art would have been motivated to perform such a modification to authenticate the user, as taught by Schneier (page 52). As modified, Lee lacks streaming decryption logic. However, Ciacelli teaches the concept that encrypting a data stream, one ensures that the information in the stream (such as copyrighted material) is not exposed during the data transfer (col. 3 lines 25-64). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to include streaming decryption logic to receive and decrypt data using the received key. One of ordinary skill in the art would have been motivated to perform such a modification to ensure that the content is not exposed during data transfer, as taught by Ciacelli (col. 3 lines 25-64).

Regarding claim 21, Lee discloses the decryption key being a content decryption key (col. 9 line 63 – col. 10 line 3) and, as modified by Ciacelli, a session key (defined by Schneier as a key used with symmetric algorithms to secure message traffic (page 33)).

6. Claim 25, as best understood, is rejected under 35 U.S.C. 103(a) as being unpatentable over **Yaegashi** in view of **Ciacelli**. Yaegashi discloses a reader (col. 9 lines 20-28) to read an

identification (col. 9 lines 1-10) and content/sensitive information (col. 8 lines 61-67) from a secure medium/distribution CD (col. 9 lines 1-10), an authentication logic to receive authentication/decryption key from the server indicating approval to read the content of the secure medium (col. 9 lines 20-38), sending the content to an application/information access system (col. 9 lines 50-59 & Fig. 1) and key logic to receive a decryption key from the server if the user is authenticated (col. 11 lines 1-22). Yaegashi discloses determining if the disk ID is already associated with a user (col. 12 lines 4-17) and if the disk ID/disc identification information is not yet associated with the user, associating the user authentication data/login identity with the disk ID/disc identification information (col. 12 lines 4-17 & lines 56-61) and determining that the current user authentication matches the user (validation/authentication by determining if the user matches a key for the current disk) (col. 10 lines 47-65 & col. 12 lines 4-8) in addition to determining if a user is associated with the disk ID/disc identification information (col. 12 lines 4-17). Yaegashi lacks explicit disclosure of the application/information access system comprising a user interface to request user identification in response to a server request and to send the data received from a user to the server. However, it is inherent that such a user interface must exist to allow the user to enter access information (col. 10 lines 47-65). Yaegashi further lacks an encryption logic further to encrypt the content prior to sending the content to an application and a streaming decryption logic to receive data from the secure device and decrypt the data using the key received and play the data. However, Ciacelli teaches the concept that encrypting a data stream, one ensures that the information in the stream (such as copyrighted material) is not exposed during the data transfer (col. 3 lines 25-64). Therefore, it would have been obvious to one having ordinary skill in the art at the time the

invention was made to encrypt the content prior to sending the content to an application and include streaming decryption logic to receive and decrypt data using the received key. One of ordinary skill in the art would have been motivated to perform such a modification to ensure that the content is not exposed during data transfer, as taught by Ciacelli (col. 3 lines 25-64).

7. Claim 26, as best understood, is rejected under 35 U.S.C. 103(a) as being unpatentable over **Yaegashi & Ciacelli**, as applied to claim 25 above, in further view of **Schneier**. Yaegashi, as modified above, lacks session key generation logic to generate a one-time session key and sending the session key encrypted to a server. However, Schneier teaches that session keys are used to secure a single conversation (p. 180) and are usually first exchanged and then used (p. 33) because symmetric encryption is faster (p. 33). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to generate a one-time session key and send it encrypted to the server. One of ordinary skill in the art would have been motivated to perform such a modification to secure the conversation, including the received authentication, with high-speed cryptography, as taught by Schneier (pp. 33 & 180).

Conclusion

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael J. Simitoski whose telephone number is (571) 272-3841. The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m.. The examiner can also be reached on alternate Fridays from 6:45 a.m. – 3:15 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached at (571) 272-3838.

Any response to this action should be mailed to:
Commissioner of Patents and Trademarks
Washington, DC 20231
Or faxed to:
(703)746-7239 (for formal communications intended for entry)
Or:
(571)273-3841 (Examiner's fax, for informal or draft communications, please label "PROPOSED" or "DRAFT")

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571) 272-2100.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MJS
June 23, 2005

David Y. Jung
Primary Examiner
7/21/06